IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA, Plaintiff, vs. MARK RINGLAND, Defendant.	8:17CR289 GOVERNMENT'S BRIEF IN OPPOSITION TO DEFENDANT'S MOTION TO SUPPRESS

INTRODUCTION

Mark Ringland has filed a motion to suppress evidence and statements. The evidence stemmed from the application and issuance of four search warrants. Two of the warrants were issued in Douglas County Court and served upon Google, Inc. for the contents of Ringland's Gmail accounts and two phone numbers. Two federal search warrants were issued. The first was a cell-phone ping warrant on August 31, 2017, in order to locate Ringland. The second was a search warrant executed on September 1, 2017, for any digital media possessed by Ringland. During the execution of the September 1, 2017, warrant, Ringland provided a detailed statement which he now seeks to suppress solely as fruit of the poisonous tree relating back to the state and federal search warrants.

Ringland is not entitled to relief. His request for a hearing under Franks v. Delaware, 438 U.S. 154 (1978) is insufficient. There were no material omissions in any of the warrant applications. Moreover, his claimed omission, that there were numerous IP addresses in the CyberTips resolving to other places and subscribers, was not significant to the determination of probable cause. Even if it was, a statement to the effect that mobile phones have rapidly changing IP addresses, would neither have added nor detracted from a determination of probable

cause. Finally, Ringland's reliance on United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016) is both factually and legally misplaced.

Facts

The facts necessary to the analysis of Ringland's claims are found in the Probable Cause sections of the federal warrant applications. In summary, the affidavit in support of the search warrants set forth a total of 19 CyberTip Reports from Google. Ultimately, those CyberTips were linked to Gmail accounts belonging to Ringland. It is the link to his email accounts, as opposed to the IP addresses that support the requisite probable cause in each warrant.

On April 17, 2017, the National Center for Missing and Exploited Children (NCMEC) provided seven CyberTip Reports relating to information received from Google stating that a user of their services had uploaded over 700 files suspected of depicting sexually explicit conduct involving a minor. The user email address was mringland69@gmail.com. The affidavit clearly states that "several IP addresses provided by Google were associated with the uploaded files, [listing two such address] and that NCMEC traced several of the addresses to Sprint PCS in Omaha, Nebraska." Thus, a preservation letter was sent to Google for the mringland69@gmail.com account.

On June 23, 2017, another CyberTip Report was provided by Google to NCMEC. This report indicated that two files suspected of depicting sexually explicit conduct involving a minor were uploaded by a user of their services. Google reviewed 502 files from the submitted CyberTips. The affiant to each warrant, C.J. Alberico of the Nebraska State Patrol, viewed those files that Google had earlier examined and forwarded to NCMEC to confirm that the images depicted child pornography. Three of those images reviewed by Google, and in turn by Investigator Alberico, were described in the affidavit. There is and can be no question that the

three images described in the affidavit depict minors engaged in sexually conduct, i.e. child pornography.

The eight CyberTips received prior to June 23, 2017, resulted in Investigator Alberico seeking a Douglas County Court search warrant to Google for information associated with the email account mringland69@gmail.com. On July 14, 2017, Google responded to the state search warrant. In reviewing the Google response, a second email address, mringland65@gmail.com, was discovered. It was determined that this second email address, mringland65@gmail.com, had sent images of child erotica and images of child pornography to the mringland69@gmail.com address. At the same time, the South Dakota Bureau of Criminal Investigation contacted Investigator Alberico to advise that they had received additional information from NCMEC regarding Google CyberTip Reports. A review of the CyberTip Reports sent to South Dakota revealed that the email address and phone number Google reported were different than the earlier CyberTips. These reports list email addresses markringland65@gmail.com and mringland69@gmail.com and a different phone number 402-306-0902. Again, Google identified several IP addresses with the uploaded files to include several resolving Sprint PCS including the Omaha area. Google provided the name Mark Ringland as the subscriber of the two email addresses, mringland69@gmail.com and mringland65@gmail.com.

On July 20, 2017, a subpoena to Sprint identified the number's subscriber as Mark Ringland, residing at an address in Bellevue, Nebraska. A preservation letter was sent to Google regarding the mringland65@gmail.com account as well as the phone number Sprint resolved to Ringland.

On August 7, 2017, nine more CyberTip Reports were received from NCMEC. These Google reports involved 1,109 files suspected of depicting sexually explicit conduct involving a

minor. The reports were all associated with the email address markringland65@gmail.com. Again, NCMEC traced some IP addresses to Sprint PCS and included the Omaha, Lincoln, and Grand Island, Nebraska, areas.

Ringland was researched in the Nebraska Criminal Justice System (NCJIS). A vehicle was found registered to Ringland to the address at 16406 Taylor Street in Omaha, Nebraska. Nebraska Department of Labor records indicated employers in Alma, Nebraska, and Grand Island, Nebraska.

On August 7, 2017, a second Douglas County Court search warrant for Google was granted. This warrant sought email addresses for mringland65@gmail.com and markringland65@gmail.com associated with his phone. On August 18, 2017, Google provided the information requested in the second Douglas County search warrant. Several of the files provided by Google contained images and videos of suspected child pornography, to include bestiality. Investigator Alberico also viewed screenshot images of child erotica.

On August 31, 2017, Investigator Alberico sought and was granted a federal search warrant for Ringland's phone. The warrant sought a "ping order" to track the location of the phone from August 31, 2017. The results of the ping order revealed that the phone was at the same address Ringland had previously registered a vehicle.

Agents went to the address indicated by GPS in northwest Omaha. Ringland's vehicle was observed near the residence. Ringland was located and the search warrant for his device was executed. Ringland was read his rights and consented to an interview and the search of other devices. During the course of his interview, Ringland indicated that he was the only person with access to his cellphone, email accounts, and passwords. He indicated that the cellphone seized by the agent had been his for approximately three months. He indicated that he had a

disease but would not actually hurt a child. He indicated that he "just observed and looked" and further admitted to saving images, but not videos of children. He indicated that he never grew out of liking children and expressed a preference for 12-13-year-old girls. Ringland indicated that he found an Internet site "no nude" and has been addicted for seven years. He would use Bing or Yahoo to search for photographs using this site and would download images and email these images to himself.

ARGUMENT

Ringland's Franks Challenge Fails

The Fourth Amendment requires that a search warrant be issued upon a showing of probable cause. United States v. Williams, 477 F.3d 554, 557 (8th Cir. 2007). To challenge a finding of probable cause under Franks, a defendant must show, by a preponderance of the evidence, that: (1) in preparing the affidavit supporting the search warrant, the affiant deliberately and knowingly, or with reckless disregard for the truth, included falsehoods; and (2) the affidavit, if supplemented by the omitted information, could not support a finding of probable cause. Franks v. Delaware, 438 U.S. 154, 171–72 (1978).

"To obtain a Franks hearing a defendant must make a substantial preliminary showing that there was an intentional or reckless false statement or omission which was necessary to the finding of probable cause, a requirement which is 'not easily met.'" United States v. Snyder, 511 F.3d 813, 816 (8th Cir. 2008). To obtain a Franks hearing, Ringland must make a substantial preliminary showing that the affidavit contains a material false statement by the affiant which is deliberately false or made with reckless disregard for the truth.

"A showing of deliberate or reckless falsehood is 'not lightly met.'" United States v. Wajda, 810 F.2d 754, 759 (8th Cir. 1987). "Allegations of negligence or innocent mistake will

not suffice." United States v. McIntyre, 646, F.3d 1107, 1114 (8th Cir. 2011). A statement is made with reckless disregard for the truth if "after viewing all the evidence, the affiant must have entertained serious doubts as to the truth of his statements or had obvious reasons to doubt the accuracy of the information he reported." United States v. Butler, 594 F.3d 955, 961 (8th Cir. 2010). Furthermore, to meet his burden of proving intentional or reckless inclusion of false statements in a warrant affidavit, "plaintiffs cannot respond with general attacks upon defendants' credibility, but must present affirmative evidence of bad motive or of a personal stake in the matter." Morris v. Lanpher, 563 F.3d 399, 403 (8th Cir. 2009). Plaintiffs must offer specific, non-conclusory evidence that a defendant police officer believed his affidavit was false or recklessly misconstrued facts. Id.

Ringland does not and cannot claim a false statement or reckless disregard for the truth of the matters asserted in the affidavit. Instead, Ringland suggests that Investigator Alberico omitted material information "that there were other geographic locations and internet protocol (IP) addresses associated with images outlined in the NCMEC CyberTipline reports." Ringland's argument fails.

To prevail on his Franks argument, Ringland grossly overstates the importance of an IP address in the probable cause determination in the instant case. There is no question that IP addresses are important in peer-to-peer cases and other computer investigations. They are less helpful in a smartphone or mobile device investigation. The mobility of the phone, in this case Ringland was later discovered to live a transient lifestyle, renders the use of an IP address less useful. Hence, the necessity for a ping order to find Ringland and his phone. Moreover, because mobile phones and devices access dynamic IP addresses so frequently, many ISPs are unable to track a specific IP to a specific phone at a specific time.

By overemphasizing reliance on the IP addresses, Ringland's argument fails to focus on how the affidavits provided probable cause. The probable cause link was based on the Gmail accounts namely: mringland69@gmail.com; mringland65@gmail.com; and markringland65@gmail.com. It is the use of these accounts that generated the CyberTips. The CyberTips included the sexually explicit images and/or erotic images involving children that caused Google to capture the image and provided the CyberTips to NCMEC. Thus, whether downloading suspect images from a website or transferring them from one Gmail account to another, probable cause was generated by the activity involving Ringland's Gmail accounts.

Ringland's argument that the applications omitted other geographic locations based upon IP addresses received Sprint fails for the same reasons. Again, the probable cause is not driven by the IP addresses. Moreover, that an IP address could be used in multiple geographic locations in connection with a mobile phone does not rule out that the phone itself traveled or, more likely, that the IP address was rapidly transferred from one mobile device to the next by the Internet Service Provider.

Investigator Alberico reviewed 502 of the images forwarded by NCMEC because those were the images that had already been viewed by Google. She confirmed that the images depicted child pornography. Whether the images were "uncategorized" or as described in the affidavit graphically detailing the sexual exploitation of a child is of no moment. Whether "uncategorized" or unquestionably child pornography is of no moment. The images themselves were filtered and forwarded by Google to NCMEC. Title 18, United States Code, Section 2258A requires ISPs, to include Google, to send images of suspected child pornography to NCMEC.

Ringland has failed to make a proper showing entitling him to a Franks hearing. The affidavits supporting the search warrants did not include falsehoods knowingly and deliberately

made or in reckless disregard of the truth. Even if the affidavits had included the extraneous information that Ringland suggests should have been included, probable cause still exists.

Ackerman

Ringland relies on United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016) to suggest that Google's CyberTips, forwarded to NCMEC, were warrantless searches is both legally nd factually flawed.

The Fourth Amendment protects persons against unreasonable searches and seizures in their "persons, houses, papers, and affects." "The basic purpose of this Amendment . . . is to safeguard the privacy and security of individuals against arbitrary invasions by government officials." Camara v. Mun. Court of City & Cty. Of San Francisco, 387 U.S. 523, 528 (1967). The Fourth Amendment is inapplicable "to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any Government official." United States v. Jacobsen, 466 U.S. 109, 113 (1984). Multiple Circuit Courts of Appeal have addressed the question of whether electronic service providers or (ESP), like Google, act as government agents when they monitor their users' activities on their servers, especially when filtering images of child engaged in sexually explicit conduct. These courts uniformly conclude that these searches are private searches and not government searchers. In United States v. Cameron, 699 F.3d 621, 638 (1st Cir. 2012), the First Circuit held that when Yahoo! chose to implement a policy to search for child pornography, it presumably did so for its own interest. The Eighth Circuit, in United States v. Stevenson, 727 F.3d 826 (8th Cir. 2013), observed the AOL's decision on its own initiative to ferret out child pornography does not convert the company into an agent or instrument of the government for Fourth Amendment purposes . . . AOL's voluntary efforts to achieve a goal that

it shares with law enforcement do not, by themselves, transform the company into a government agent. Id. at 831. The Fourth Circuit in United States v. Richardson, 607 F.3d 357 (4th Cir. 2010), held that AOL's scanning of email communications for child pornography did not trigger the Fourth Amendment warrant requirement because no law enforcement officer or agency asked the provider to search or scan the defendant's emails. Id. at 366; See also, United States v. Stratton, 229 F. Supp. 3d 1230, 1243 (D. Kan. 2017) (compiling cases).

Ringland relies on United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016) to suggest that Google, in the first instance, by searching for child pornography and reporting it to NCMEC, and NCMEC by providing those tips to law enforcement, become government actors and thus violate the Fourth Amendment. However, Ackerman is factually distinct from the present case and therefore Ringland's legal argument has no merit.

The defendant in Ackerman used AOL to send email containing child pornography. An email containing child pornography was intercepted by an automated filter designed to detect and stop the transmission of child pornography. Once AOL detected the image, it halted delivery and reported the email to NCMEC. Nobody from within AOL actually opened or reviewed the child pornographic images before referring them to NCMEC.

When the CyberTip from AOL was received at NCMEC, a NCMEC analyst viewed the images, one that AOL had flagged through its filter and three that were not so identified, and determined that all four images were in fact child pornography. The Tenth Circuit found that by examining images that AOL had not previously examined, NCMEC exceeded AOL's private search and held that NCMEC had violated the defendant's Fourth Amendment rights. Ackerman, 831 F.3d at 1306–07.

Ringland's case is not Ackerman. NCMEC changed its rules and procedures in response to the Tenth Circuit's decision in Ackerman. NCMEC will not view an image that was not previously viewed by the Electronic Service Provider. Thus, when NCMEC receives an image that has previously been reviewed by an ESP, it will forward the image or images that have been reviewed via private search to law enforcement. When an Electronic Service Provider such as Chatstep forwards images solely based on photo DNA, without physically examining the images themselves, NCMEC will not view the image. It will forward the referral to law enforcement who will then seek a search warrant to view the non-examined images.

In the present case, it is clearly set forth in the affidavits that Google had examined and viewed some of the images forwarded but not all. Hence, in her affidavit, Investigator Alberico stated:

> Provided with the eight (8) total CyberTip Reports, were one thousand two hundred sixteen (1,216) files that contained alleged contraband. Google reviewed five hundred and two (502) files from the CyberTips submitted. Your affiant viewed the same files that Google reviewed and confirmed the images depicted child pornography. . .

Thus, that which had been reviewed by Google prior to being forwarded to NCMEC were the images reviewed by Investigator Alberico prior to obtaining search warrants for the email accounts. Thus, neither NCMEC nor Alberico's review exceeded the private search of Google.

Good Faith

The good-faith exception to the Fourth Amendment was established in United States v. Leon, 468 U.S. 897 (1984). "[i]f the purpose of the [Fourth Amendment's] exclusionary rule is to deter unlawful police conduct, then evidence obtained from a search should be suppressed only if it can be said that the law enforcement officer had knowledge or may be properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment." Id.

at 919. The exclusionary rule deters deliberate, reckless, or grossly negligent conduct. Herring v. United States, 555 U.S. 135, 144 (2009).

In the present case, law enforcement did not violate Ringland's Fourth Amendment rights. If, only for the sake of argument, Ringland's Fourth Amendment rights were violated, there is nothing to suggest that law enforcement acted in a deliberate, reckless, or grossly negligent fashion to violate the Fourth Amendment rights of Ringland. Google conducted a private search and law enforcement had no reason to believe otherwise. The results of the private search were provided to NCMEC. NCMEC then referred those images, suspected of being child pornography, to the Nebraska State Patrol. The images that had previously been examined and reviewed by an employee at Google were then reviewed by Investigator Alberico and used to obtain search warrants for three email accounts of Ringland. Thus, the agents viewed what was available through a private search, used it to provide probable cause for a court-authorized search warrant, and thus received the email contents of Ringland's accounts from Google. Law enforcement's conduct was wholly appropriate and nothing is accomplished by use of the exclusionary rule. See, Stratton, 229 F. Supp. 3d at 1243.

CONCLUSION

For the reasons stated above, the United States respectfully submits that defendant's request for a Franks hearing be denied as he has failed to make the requisite showing. Moreover, the United States respectfully requests that the motion to suppress evidence and statements be denied.

UNITED STATES OF AMERICA, Plaintiff

JOSEPH P. KELLY
United States Attorney
District of Nebraska

By: *s/ Michael P. Norris*
MICHAEL P. NORRIS (#17765)
Assistant U.S. Attorney
1620 Dodge Street, Suite 1400
Omaha, NE 68102-1506
Tel: (402) 661-3700
Fax: (402) 661-3084
E-mail: Michael.Norris@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on May 3, 2018, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which sent notification of such filing to all registered participants. I also hereby certify that a copy of the same was served by regular mail, postage prepaid, to the following non-CM/ECF participants:

s/ Michael P. Norris
Assistant U.S. Attorney